ORIGINAL

United States District Court
NORTHERN DISTRICT OF GEORGIA

UNITED STATES OF AMERICA

v.

Kevin M. Sullivan

CRIMINAL COMPLAINT

Case Number: 1:15-MJ-502

I, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief. On or about June 15, 2015 in DeKalb County, in the Northern District of Georgia, defendant(s) did, knowingly possess at least one image depicting a minor engaged in sexually explicit conduct, said depiction having been produced using minors engaged in sexually explicit conduct, and having been shipped or transported in interstate commerce by any means including computer,

in violation of Title 18, United States Code, Section(s) 2252(a)(4)(B).

I further state that I am a(n) Special Agent and that this complaint is based on the following facts:

PLEASE SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof. Yes

Sara Thomas
Signature of Complainant
Sara Thomas

Based upon this complaint, this Court finds that there is probable cause to believe that an offense has been committed and that the defendant has committed it. Sworn to before me, and subscribed in my presence

June 17, 2015
Date

at Atlanta, Georgia
City and State

JANET F. KING
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer
AUSA Paul Jones

Signature of Judicial Officer

AFFIDAVIT

I, Sara R. Thomas, being first duly sworn, depose and state the following:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Georgia Bureau of Investigation (GBI) and have been so assigned since September of 2007. I am currently assigned to the Child Exploitation and Computer Crime's Unit in Atlanta, Georgia. I additionally serve in the role of a Task Force Agent with the Homeland Security Investigation's Special Agent in Charge (SAC) Office in Atlanta, Georgia. As a part of my official duties, I have conducted and participated in investigations related to the sexual exploitation of children. During the course of these investigations, I have observed and reviewed examples of child pornography in various forms of media, including computer media. As part of my duties and responsibilities as a GBI Special Agent and HSI Task Force Officer, I am authorized to investigate crimes which involve the sexual exploitation of children pursuant to Title 18, United States Code, Sections 1466A, 2251, 2252, and 2252A. I have completed the GBI Special Agent Basic Training Academy at the Georgia Public Safety Training Center, as well as the HSI Task Force Agent Training Program. I have attended hundreds of hours of training related to the sexual exploitation of children, and am a Peace Officer Standards and Training (POST) Certified Instructor for the State of Georgia. I have trained over 20,000 local, state, federal and international law enforcement officers and personnel on the subject of sexual exploitation of children. These training classes occurred throughout the United States and abroad, including Israel, Brazil, and the Republic of Georgia.

2. As part of my duties as a GBI Special Agent and HSI Task Force Agent, I have gained

experience conducting criminal investigations involving child exploitation and child pornography, and have participated in the execution of numerous search and arrest warrants in such investigations.

3. The statements contained in this affidavit are based on my experience, training, and background as a GBI Agent and HSI Task Force Agent, as well as information provided to me by other law enforcement officers involved in this investigation. Based on the included information, your affiant believes there is probable cause for an arrest warrant for KEVIN M. SULLIVAN.

4. Since this affidavit is being submitted for the limited purpose of securing an arrest warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause that a violation of Title 18, United States Code, Sections 2252(a)(4)(B) (possession of child pornography) has been committed by KEVIN M. SULLIVAN.

Background of the Investigation

5. In March of 2015, I received the following information from HSI Special Agent James Kilpatrick of the Cyber Crimes Center (C3):

6. Operation Amateur Lover (Herein referred to as OPAL) is a joint investigation by: U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) Cyber Crimes Center, Child Exploitation Investigations Unit (CEIU); the Municipal Police of Zurich, Switzerland; Federal Department of Justice and Police (FDJP), Federal Office of Police (Fedpol); and Swiss Coordination Unit for Cybercrime Control (CYCO). The Fedpol investigated a web-board picture gallery site that only partially contained material which

depicted the sexual exploitation of minors.

7. This site contained an area restricted to members which required members to register on the site to gain access to the restricted areas and to be able to upload content. Fedpol has identified more than 800 unique IP addresses associated with visitors from the United States who have downloaded 5 or more images which meet the definition of CAM (Child Abuse Material) as classified by investigators in Switzerland. The laws in Switzerland, relating to child exploitation, very closely mirror U.S. federal laws.

8. On October 9, 2014, the Municipal Police of Zurich Switzerland seized a server, which was being operated out of the residence of a subject in Zurich, Switzerland, from a Network-Attached Storage (NAS), which is a computer data storage server connected to a network that provides data access. The NAS was located in the residence. The operator of the site has been accused and charged with the possession and distribution of child pornography.

9. The Zurich Police thoroughly analyzed a board that was seized on the server and categorized every site-element. Approximately 80% of the site contains material depicting individuals over the age of 18 years, and approximately 20% of the site contains materials involving individuals under the age of 18 years. They compiled a list of visitors' Internet Protocol (IP) addresses[1] and the number of requests by visitor's IP addresses in conjunction with the picture categorization. The output of this analysis identified more than 2,600 IP addresses that resolved to the USA.

10. When Fedpol seized the data, all of the images were processed and categorized. The material

[1] An IP address is a series of four numbers separated by a period. It identifies a particular computer that is accessing the Internet. An Internet Service Provider assigns the IP address, and through the IP address a user of a computer is able to access websites on the Internet.

was categorized into 4 base categories; Non Pertinent, Child Abuse Material (CAM), NON CAM, and CGI Animation. Relevant to this affidavit, CAM was determined to be material that is appears to be child pornography—that is, children engaged in sexually explicit conduct. This consists of material that would be prosecutable in the United States as child pornography. This category includes known victims, identified victims, and material where an investigator would be comfortable testifying in court that this material appears to be child pornography as defined by statute.

11. On January 16, 2015 Fedpol provided the CEIU with access logs and content associated with 844 unique IP addresses resolving to the United States. After categorizing the material, Fedpol ran a script against the logs from the server seized pursuant to their investigation. The script identified unique IP Addresses that met one of two criteria: the IP address had downloaded five or more images that were CAM and were U.S.-based IP addresses or had uploaded one or more images that were CAM and was a U.S.-based IP address. Fedpol has provided the CEIU with the logs from the server for the "Get" commands associated with these transactions which documents the downloading of the particular file. Fedpol has also provided the CEIU with the actual files for the categories of CAM and NON CAM. Fedpol has also provided the CEIU with the number of get commands by IP address for the categories of CAM, NON CAM, and Non Pertinent.

12. One of the IP addresses provided by Fedpol was identified as 170.140.105.120 used from 2014-07-11 19:07:52 to 2014-08-15 20:35:44 UTC/GMT. The IP address was documented downloading the following number of images:

CAM Count: 22

NON CAM Count: 23

Non Pertinent Count: 71

All Pictures Count: 116

13. Agent Kilpatrick identified that the IP address resolved to Armstrong Cable Service, in association with Emory University in Atlanta, DeKalb County, Georgia. SA Kilpatrick submitted a federal summons to Armstrong Cable Service on February 5, 2015 for the purpose of obtaining subscriber information. Armstrong Cable Service responded to Agent Kilpatrick's summons, and identified the subscriber of the IP address as Emory University.

14. Agent Kilpatrick submitted a second Summons to Emory University to identify the user of the IP address. On March 18, 2015, Emory University responded that the IP address resolved to a wireless guest network at the university. The I.T. Security Specialist at Emory University was unable to find the name of any individual; however, he did identify the MAC address of the computer as 68:a3:c4:e2:6a:7e.[2] He also found that that MAC address continued to connect to the Emory wireless guest network logging in with bogus e-mail addresses. The Specialist was able to identify the building where the computer accesses the network.

Probable Cause

15. On Wednesday, April 1, 2015, I reviewed the files provided by Agent Kilpatrick. I located ten (10) files under the "CAM" folder.

16. I reviewed the above files and confirmed that each file consisted of an image containing a

[2] A Media Access Control (MAC) address is a hardware identification number that uniquely identifies each device on a network. The MAC address is manufactured into the device's hardware and therefore cannot be changed. A MAC address is like a serial number of a phone while the IP address is like the phone number.

lewd exhibition of prepubescent females' genitals, which constitutes sexually explicit conduct under 18 U.S.C. § 2252(a)(4)(B).

17. I contacted Lead IT Specialist Derek Spransy of Emory University's Threat, Vulnerability and Incident Management Center. Specialist Spransy advised the following:

a. The Emory IP address provided to him by Agent Kilpatrick represents many potential individual wireless users under a single IP address. In order to narrow his search, IT Specialist Spransy asked Agent Kilpatrick for the IP addresses that the domains in the summons would have resolved to on the days in question. NAT translation logs record IP addresses that were accessed, but not specific domains.[3]

b. IT Specialist Spransy then looked at Emory University's Dynamic Host Configuration Protocol (DHCP) logs and found the entry that identifies the MAC address of the computer of the relevant IP address. DHCP is the service that assigns IP addresses to clients. The MAC address was assigned to a specific IP address. The name of the computer was also identified as "Kev-HP".

c. A search of this MAC address in Emory University's wireless network logs showed the wireless access point association history of the system. As far back as their system has logs, IT Specialist Spransy identified it connecting to access points located in 401 Rollins Way, which is the Claudia Nance Rollins

[3] Network Address Translation (NAT) is a way to map an entire network to a single IP address. NAT is necessary when the total number of IP addresses assigned by the Internet Service Provider is less than the total number of computers that need access to the Internet.

School of Public Health building.

d. As a result, IT Specialist Spransy was able to determine that the MAC address of the suspect digital device in this investigation is "68:a3:c4:e2:6a:7e".

18. I contacted Agent Kilpatrick, Digital Forensics Investigator Matthew Health of the Georgia Bureau of Investigation, and Detective Jennifer Miller of the DeKalb County Police Department. Agent Kilpatrick, Investigator Heath and Detective Miller informed me that a digital device called a "sniffer" could be used to locate the wireless device containing the suspect MAC address, "68:a3:c4:e2:6a:7e".

19. I am aware, through my training and experience as a GBI Agent and HSI Task Force Agent, that computers communicate by broadcasting messages on a network using an IP address. Such networks can be on local area networks or exposed to the internet. I was informed by Detective Miller and Agent Kilpatrick that when computers access local area networks or the internet, network sniffers can be used to identify devices through the identification of their MAC address by capturing low-level package data that is being transmitted over a specific network. Agent Kilpatrick, Detective Miller, Digital Forensics Investigator Heath have been trained on how to operate sniffer devices.

20. On Tuesday, June 9, 2015, I met with Counsel Mina Rhee and Threat, Vulnerability, and Incident Management Lead Derek Spransy at Emory University's Technology and Security Office. Also present during the meeting was HSI Forensics Agent Mike Richardson, HSI Forensics Agent Chris Lehman, DeKalb County PD Detective Jennifer Miller, GBI Digital Forensics Investigator Matthew Heath, and ATF Special Agent Amy Mcleod.

21. During that meeting, Spransy informed me that the computer associated with the suspect MAC address, 68:a3:c4:e2:6a:7e, was identified as "Kev-HP". Additionally, the MAC address logged onto the guest wireless network using access points in the Claudia Nance Rollins Building, School of Public Health on a regular basis. The access points used regularly were identified as "2051" and

"3049". The access point numbers coincide with the office room numbers where the access device is located. Spransy explained that, in computer networking, a wireless access point is a device that allows wireless devices to connect to a wired network using Wi-Fi, or related standards. The wireless access point connects to a router (via a wired network) as a standalone device.

22. Spransy additionally informed me that he conducted a search for the name "Kevin" in Emory's faculty database. He identified three faculty members named Kevin. Only one of those people worked in the Claudia Nance Rollins Building. That person was identified as: Kevin M. SULLIVAN. Spransy further advised that SULLIVAN's office was located in the Claudia Nance Rollins Building, School of Public Health. His office number is "3051". Spransy stated that the access points of the office next to him, 3049, and the office below him, 2051, could be accessed very easily from office 3051.

23. On Monday, June 15, 2015, a DeKalb County Superior Court search warrant was executed at the Claudia Nance Rollins Building, School of Public Health, 3rd Flood, located at 401 Rollins Way, in DeKalb County, Georgia. As authorized by the warrant, a sniffer device was used by Detective Jennifer Miller and GBI Digital Forensics Investigator Matthew Heath to identify the wireless device associated with the suspect MAC address, "68:a3:c4:e2:6a:7e", that had been identified in this investigation. The sniffer device indicated that the MAC address was associated with a device located in office number "3051".

24. I knocked on the door of office number "3051", which was occupied by KEVIN M. SULLIVAN. SULLIVAN answered the door and exited his office. I attempted to interview SULLIVAN; however, he invoked his *Miranda* rights and left the building. A personally-owned HP laptop associated with the MAC address 68:a3:c4:e2:6a:7e was located. Attached to the HP laptop was a digital hard drive. DeKalb County Detective Jennifer Miller and GBI Digital Forensics Investigator Matthew Heath conducted a preview on the external hard drive, and located numerous files of child pornography.

25. I reviewed the files located by DFI Matthew Heath. The files displayed the genitals of prepubescent females. For example, "1322747222140.jpg" was a still image that depicted a prepubescent female, approximately four to seven years of age, with her legs spread and her vagina showing.

26. The following digital devices and items were seized from SULLIVAN's office for the purpose of completing a full forensic examination at the GBI and HSI Forensic Laboratories: External Hard Drive (model 90000-40479-002); HP Laptop (model 2000); Toshiba 16 GB Flash Drive; Sony 128 MB black Flash Drive; Compaq Presario Laptop (model V2000); Dell All-In-One Computer; iPhone 6; orange in color Flash Drive with unknown storage capacity; Microsoft tablet; and miscellaneous DVDs/CDs.

27. DeKalb County Detectives T. L. Kennedy and Jeremy Stahl located SULLIVAN at his residence. The residence was located at 1531 North Amanda Circle in Atlanta, DeKalb County, Georgia. At that time, they determined that SULLIVAN was attempting to delete/destroy evidence of child pornography on digital devices inside the residence. SULLIVAN was taken into custody by Detective T. L. Kennedy and Detective Jeremy Stahl.

28. On Monday, June 15, 2015, a Superior Court Search Warrant was executed at SULLIVAN's residence, 1531 North Amanda Circle in Atlanta, DeKalb County, Georgia. As a result, a desktop computer and Apple iPad tablet were seized.

29. GBI DFI Matthew Heath confirmed that SULLIVAN attempted to perform a defragmentation on the desktop computer. GBI DFI Matthew Heath advised that the defragmentation process can be used to delete/hide information because it compromises and reorganizes data on the device, making it more difficult to recover deleted files during a forensic examination.

Conclusion

30. Based on the foregoing facts and statements, I believe that there is probable cause to believe that KEVIN M. SULLIVAN has knowingly possessed at least one image depicting a minor

engaged in sexually explicit conduct, said depiction having been produced using minors engaged in sexually explicit conduct, and having been shipped or transported in interstate commerce by any means including computer, in violation of 18 U.S.C. § 2252(a)(4)(B).